AO 106 (Rev. 04/10) Application for a Search Warrant HH/EC

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information, inlcuding content of Apple iCloud accounts associated with emails accounts BERNIEJAKITS@ME.COM and BERNIEJAKITS@COMCAST.NET,previously stored at Apple, Inc. and currently held at the FBI in Columbus, Ohio.

Case No. 2:22-mj-808

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 875, 1465	Extortion, Production of obscenity for interstate distribution
18 U.S.C. 2251	Production/Making a notice or advertisement seeking to receive child pornography
18 U.S.C. 2252 and 2252A	Possession, distribution, and/or receipt of child pornography
18 U.S.C. 2422 (b)	Attempted coercion or enticement of a minor to engage in illegal sexual activity

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Andrew D. McCabe, FBI SA
Printed name and title

Sworn to before me and signed in my presence.

Date: December 22, 2022

City and state: Columbus, Ohio

Kimberly A. Johnson
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF:	)	
	)	
Information, including the content of communications contained in the iCloud account that is associated with emails accounts BERNIEJAKITS@ME.COM and BERNIEJAKITS@COMCAST.NET that was previously stored at the premises controlled by Apple Inc., and is currently held at FBI secure evidence Storage, 425 W. Nationwide Blvd, Columbus, Ohio	)	**Case No.** 2:22-mj-808
	)	**Magistrate Judge:**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Andrew D. McCabe, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I am a Special Agent with the FBI assigned to the Cincinnati Division, Cambridge Resident Agency and I have been a Special Agent since September 2010. During my tenure as an FBI Special Agent, I have investigated numerous crimes including, but not limited to, bank robbery, drug trafficking, racketeering, kidnapping, violent extremism, and crimes against children.
2. While performing my duties as a Special Agent, I have participated in various investigations involving computer-related offenses and have executed search warrants, including those involving searches and seizures of computers, digital media, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses. As part of my duties as a Special Agent, I investigate various criminal child exploitation offenses, including those in violation of 18 U.S.C. §§ 2251, *et seq* and 2421, *et seq*.
3. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The property to be searched is the content of the iCloud account associated with the email addresses berniejakits@me.com and berniejakits@comcast.net, which was provided to the FBI pursuant to a search warrant issued in April of 2020 and which has been stored on a digital media device in secure evidence storage since the time of its provision by Apple. Pursuant to the previously issued search warrant, the content has been searched for evidence pertaining to violations of 18 U.S.C. §§ 2252, 2252, and 2422(b). The evidence currently sought to be searched for is described in the following paragraphs and in Attachments A and B.

5. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have set forth only the facts necessary to establish probable cause for a search warrant for the content of the iCloud account associated with the Apple IDs berniejakits@me.com and berniejakits@comcast.net (the **SUBJECT ACCOUNTS**). I have not omitted any facts that would negate probable cause.

6. The **SUBJECT ACCOUNTS** to be searched are more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits and evidence of violations of 18 U.S.C. §§ 875(d), 1465, 2251, 2252 and 2422(b) – interstate extortion, production of obscenity for interstate distribution, production, advertising/solicitation for/or, and receipt of visual depictions of minors engaged in sexually explicit conduct (hereinafter "child pornography"), and the coercion or enticement of a minor(s). I am requesting authority to search the entire content of the **SUBJECT ACCOUNTS,** wherein the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

III. APPLICABLE STATUTES AND DEFINITIONS

7. Title 18, United States Code, Section 875(d) makes it a federal crime for any person to, with intent to extort any money or other thing of value from any person, transmit in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or any of another, or a threat to accuse the addressee or any other person of a crime.

8. Title 18, United States Code, Section 1465 makes it a federal crime for any person to knowingly produce with intent to transport or to transport in interstate commerce, for the purpose of selling or distributing, any obscene matter.
9. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.
10. Title 18 United States Code, Section 2251(d)(1)(A) makes it a federal crime for any person to make, print, publish, or cause to be made, printed or published, any notice or advertisement that seeks or offers to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction involving the use of a minor engaging in sexually explicit conduct, if such person knows or has reason to know that either the notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail; or that the notice or advertisement actually was transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.
11. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce, or is in or affecting interstate commerce.
12. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to

knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

13. Title 18, United States Code, Section 2422(b), makes it a federal crime for any person to knowingly use a means of interstate commerce to persuade, induce, entice, or coerce or attempt to persuade, induce, entice or coerce, any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person may be charged with a crime. Production of child pornography as defined in 18 U.S.C. § 2251(a) is included in the definition of sexual activity for which any person may be charged with a crime.

14. As it used in 18 U.S.C. §§ 2251 and 2252, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2) (A) as: actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

15. As it is used in 18 U.S.C. § 2252A(a)(2), the term "child pornography"[1] is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

16. The term "sexually explicit conduct" has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), "sexually explicit conduct" also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse,

[1] The term child pornography is used throughout this affidavit. All references to this term in this affidavit, and Attachments A and B hereto, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated; (i) bestiality; (ii) masturbation; (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

17. The term "minor", as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as "any person under the age of eighteen years."

18. The term "graphic," as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean "that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted."

19. The term "visual depiction," as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.

20. The term "computer"[2] is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

21. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

22. "Internet Service Providers" (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

23. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP

[2] The term "computer" is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

IV. INFORMATION REGARDING APPLE ID AND ICLOUD[3]

24. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

25. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

    a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

    b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

    c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

    d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store

3 The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

26. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

27. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime)

only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

28. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

29. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

30. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play

content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

31. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.
32. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the offenses under investigation, or, alternatively, to exclude the innocent from further suspicion.
33. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, photos, and videos, are often created and used in furtherance of criminal activity, including communicating and facilitating the offenses under investigation.
34. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan

to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

35. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal other platforms used by JAKITS to communicate with minors or extort adults to produce obscenity or to send obscenity to adults. In addition, emails, instant messages, Internet activity, documents, and contact information can lead to the identification of additional victims, other co-conspirators, and instrumentalities of the crimes under investigation.

V. INVESTIGATION AND PROBABLE CAUSE

36. In October of 2022, Bernhard Jakits was indicted in the Southern District of Ohio on three counts of sexual exploitation of a minor by the production or attempted production of child pornography, in violation of 18 U.S.C. § 2251(a); one count of sending a notice seeking minors to engage in sexually explicit conduct for the purpose of producing a visual depiction, in violation of 18 U.S.C. § 2251(d)(1)(B); one count of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2); two counts of coercion or enticement of a minor, in violation of 18 U.S.C. § 2422(b); and one count of interstate communications with intent to extort, in violation of 18 U.S.C. § 875(d). This indictment was the result of an investigation by your affiant and the Belmont County Sheriff's Office (BCSO), which is summarized below.

37. In or about January of 2020, you affiant received information from the BCSO regarding an individual who had solicited nude photographs of two minor females residing in Belmont County. According to the information provided by BCSO, A.M., and adult female, had turned herself into authorities in mid-January of 2019 to resolve various legal issues related to prostitution and other similar activities. Once in the Belmont County jail, A.M. reached out to detectives regarding her concern about her minor daughters. A.M. stated that when she had been engaged in prostitution, she had met a man named Bernhard Jakits online. She sent images of herself to Jakits, who lived in Maryland, in exchange for money that he sent her through Western Union. During her interactions with Jakits, he asked about her daughters, but she would divert the conversation away from them. However, according to the A.M, her oldest daughter intercepted a text message from Jakits on A.M.'s phone while she was

sleeping. It was shortly after this interaction that the mother turned herself into authorities, and, since she had left her phone in her home, she was concerned that her daughters had been in contact with Jakits.

38. As a result of A.M.'s statements, forensic interviews were conducted of the two daughters. The eldest daughter (hereinafter Victim 1), who was born in 2003 and was 15 years old at the time of the interview, revealed that she had sent nude photographs of herself to an adult male that she knew by the names Mr. Wow and Bernie. She further stated that she had informed Bernie of her age. According to Victim 1, Bernie had also tried to convince both her and her younger sister (hereinafter Victim 2, who was born in 2005 and was 13 years old at the time) to video chat with him in exchange for money. During the interview of Victim 2, Victim 2 stated that she sent photos to a man that she knew as either Mr. Wow or Wild. She did not know his true name. She confirmed that Mr. Wow was aware of her age and the age of Victim 1, and that he solicited photos of them either nude or in their bras and underwear. Victim 2 admitted that she sent Mr. Wow three pictures of herself, including pictures of her nude, in exchange for money he had offered them. She also reiterated Victim 1's statement that Mr. Wow had sought to video chat with them in exchange for money, but that they had declined to do so.

39. At the time of the interviews with Victim 1 and Victim 2, their guardian turned over three cellular telephones to BCSO which were believed to have been used to communicate with Jakits. Phone 1 was a pink iPhone 8 belonging to Victim 1. Phone 2 was a Samsung Galaxy J7 Prime Cellular Telephone which belonged to A.M. Phone 3 was an Alcatel Tracphone Model A574BL which belonged to Victim 1 and Victim 2's grandmother and was utilized at times by Victim 2. A BCSO detective reviewed the contents of Phone 1, Victim 1's iPhone, and confirmed that it contained several nude images of Victim 1 and Victim 2, as well as images of them holding up school transcripts and or prescriptions that clearly showed their ages. In addition, a chat thread with a contact named Mr. Wow was recovered which depicted some of the above-noted images being sent in conjunction with discussions about the money the victims would receive for such pictures. The chat thread listed the phone number for Mr. Wow as (443) 742-1792.

40. The BCSO identified the subject described by Victim 1, Victim 2 and A.M. as a Bernhard Jakits, residing at 15 Spa Creek Landing, Annapolis, MD, 21403 by conducting an open-source data base check on telephone number (443) 742-1792. In addition to their

investigative reports detailing all of the foregoing information, BCSO provided your affiant with the three aforementioned cellular telephones.

41. On January 22, 2020, your affiant conducted an interview of A.M to obtain further information regarding her interactions with Jakits. A.M. self-admitted to being a prostitute and using the website, "Skip the Games," to meet clients. A.M's Skip the Games profile included her photographs and a telephone number. On an unspecified date, Jakits contacted A.M. and began an online relationship with her using the video messaging service Duo. Jakits sent money to the mother utilizing Western Union, and in exchange A.M. sent Jakits photos and videos of her preforming sexually explicit activities. As the relationship between A.M. and Jakits continued, Jakits would ask A.M. to perform more degrading acts, including bestiality. When A.M. refused, Jakits showed her images taken from her own videos. Jakits stated he would send the photos to A.M.'s family member and other associates if she did not comply with his additional requests. In addition to photographs of A.M., Jakits showed her images he had of other women engaged in sexually explicit actions. In December 2018, Jakits learned A.M. had two minor daughters. Jakits began asking A.M. to introduce him to her daughters, Victim 1 and Victim 2. A.M. informed Jakits that Victim 1 and Victim 2 were juveniles, and he should not message them. After she turned herself into BCSO in January 2019, she received money on her books from a friend, which she knew to be Jakits. Also knowing that Jakits would not send her money for no reason, A.M. became concerned about him communicating with Victim 1 and Victim 2. After a conversation with her daughters in which they confirmed they communicated with Jakits and sent him nude pictures in exchange for money, A.M. reached out to BCSO detectives and provided this information.
42. During the interview with your affiant, A.M. identified a publicly available photograph of Bernhard Jakits obtained from roguewaveyachtsales.com website, as the man with whom she had been communicating. The website also listed (443) 742-1792 as Jakits' telephone number. A.M. also provided consent to search the three aforementioned cellular phones. Your affiant thereafter submitted all three cellular phones to the FBI forensic examination laboratory and requested that they be forensically examined.
43. In January 2020, a subpoena was issued to Verizon wireless for subscriber information related to the phone number (443) 742-1792. Responsive information provided by Verizon identified the subscriber of (443) 742-1792 as Bernhard Jakits, P.O. Box 5015, Annapolis, MD. Furthermore, Verizon identified the device IMEI number as 353824089666214. A check of a

commercially available internet site that collects IMEI information determined that the aforementioned IMEI Number is associated with an Apple iPhone 7 cellular telephone.

44. In February of 2020, the Cincinnati FBI conducted Cellebrite forensic extractions of the three cellular telephones utilized by Victim 1, Victim 2, and A.M. Your affiant received and reviewed the forensic extractions of the phones and located 179 TextNow messages on Victim 1's iPhone between Victim 1 and the phone number (443) 742-1792 that is associated with Jakits, between approximately January 14 and 21, 2019. The following are excerpts from the communications recovered from Victim 1's phone that occurred on or about January 14, 2019:

- VICTIM 1: This is [Victim 1]
- JAKITS: Then call me and I'll tell you.
- Four-minute call to Victim 1.
- JAKITS: Also important,,,Ask your sister if she wants to earn $500 also 8:00PM tonight Talk then.
- JAKITS: Got another idea Please call me.
- JAKITS: You there?
- VICTIM 1: I can't call I'm wit [sic] a friend now.
- JAKITS: Thanks for letting me know. Have fun. We'll speak later this evening. Remember to ask your sister.
- JAKITS: Hi....Did you ask your Sister yet?
- VICTIM 1: I'm at a friends staying the night so no I didn't ask her.
- JAKITS: Please ask her when you can And how about what we have planned for later
- VICTIM 1: It's still on
- JAKITS: Oh goodie
- JAKITS: Its almost 8pm dear
- JAKITS: [Victim 1][], I just sent your Mom more money to make her stay there a little more pleasant
- JAKITS: Its 8pm honey
- JAKITS: ???
- JAKITS: Did you fall asleep? I didn't...
- JAKITS: [VICTIM1][], you need to become a lot more responsible if you want my help
- VICTIM 1: I am responsible sometimes I'm just not in the mood to go through all this shit with u

45. The following are excerpts from the communication recovered from Victim 1's phone that occurred on or about January 15, 2019:

- JAKITS: Are you up to making some money?
- JAKITS : $1000
- VICTIM 1: Yea

***

- JAKITS: Good When?
- VICTIM 1: When ever u want to
- JAKITS: 9:00pm sharp… Also, have you spoken to your sister, if so, $500 for her
- VICTIM 1: So how much am I getting and how much would she be if she said yes
- JAKITS: $1000 for your time $500 for your Sister's time
- VICTIM 1: Okay
- JAKITS: Okay what
- VICTIM 1: Okay as in we both r in
- JAKITS: Yes definitely I'd like to see what your sister looks like please
- VICTIM 1 sent Photograph 1, depicting two clothed minor females posing in front of a mirror, Photograph 2, depicting two clothed minor females lying on a bed, and Photograph 3, also depicting two clothed minor females lying on a bed, as text message attachments.
- VICTIM 1: She's the one with the curly hair
- JAKITS: Cute Very very cute both of you Before we start We need to promise that its our secret. This is as far as it goes...i promise Now one naked picture of your sister, after that we'll plan our party
- VICTIM1: Rn?

***

- JAKITS: Yes
- VICTIM 1 sent Photograph 4, an image of a young naked female holding a cellular phone. Both the female's breasts and pubic region are clearly visible.
- JAKITS: Well, whats happening? Plus with face of your sister
- VICTIM 1: I sent it
- JAKITS: Cute Have also show her school transcript Then you call me and i'll tell you what i want
- VICTIM 1: She hasn't got hers yet
- JAKITS: Have hold something up with her name on it
- VICTIM 1 sent Photograph 5 an image of a fully clothed female holding prescription from East Ohio Regional Hospital. The prescription shows VICTIM2's name and her date of birth
- JAKITS: Cute Now call me
- VICTIM 1 made a four-minute call to JAKITS.

***

- VICTIM1: What r u asking for on ft
- JAKITS: That she model and do certain things Nothing nasty I promise
- JAKITS: Plus a couple of pictures that i want her to take of how i want it
- VICTIM1: Okay

***

- JAKITS: It's 9 o'clock
- Incoming unanswered call to Victim 1 from Jakits

- VICTIM1: We're gonna have to wait a little longer my gma is in the room and someone is in the bathroom
- JAKITS: Hate waiting but i will

***

- VICTIM 1: So this is what we're doing . We're gonna do all the pictures first me and my sister and then we will ft so it can go faster and be over with
- JAKITS: Its not a bad plan You'll poise [sic] in the ways that i want you two to do Then if happy, we'll ft and finish it off How does that sound?
- VICTIM 1: Great
- JAKITS: Lets start sooner than later
- VICTIM 1: Waiting on u
- JAKITS: I'm here
- VICTIM 1: Okay so tell me the poses
- JAKITS: Call me and i'll tell you
- VICTIM 1: Just text me them I've got a lot of homework to do so I wanna do this quick
- JAKITS: First your sister Have her call me Don't want to write/text it
- JAKITS: Then you Tomorrow morning you guys will have $1500
- VICTIM 1 made a one-minute call to Jakits

***

- VICTIM 1: We don't rlly feel comfortable FaceTiming you so... idk
- JAKITS: $1500
- JAKITS: Its that or nothing I'm soon need to do other things, hope that you understand 1000 for you 500 for your sister Soon i'm leaving Because I have other obligations
- JAKITS: Facetime or google duo Its that or nothing

***

- JAKITS: One thousand five hundred dollars is a lot of money Think hard and long [Victim 1][]
- JAKITS: Remember that i can get more screwed with this than you can Yes or no or i'm going out Thanks either way

***

- JAKITS: Both of you facetime No bullshit $1000 a piece
- VICTIM 1: What do we have to do on FaceTime is my question
- JAKITS: Whatever i tell you
- JAKITS: Nothing nasty I ain't and don't like nasty
- JAKITS: If you're thinking about it, Then show me a close-up of both of your bottoms Simple It's a lot of money

***

- VICTIM1: We don't . Feel comfortable doing it[.]

46. In further communications recovered from Victim 1's phone that continued through on or about January 21, 2019, Jakits continued to tell Victim 1 that he would provide Victim 1,

Victim 2, and A.M. with a lot of money, claiming that he was a millionaire, asking if they were "up for trying again" or if Victim 1 would answer him. Victim 1 did not respond to any of Jakits' messages.

47. Numerous photos were also recovered from the phone belonging to Victim 1. These photos depicted a young Hispanic female in various states of undress, including close up nude images of female genitalia.

48. On or about March 10, 2020, an administrative subpoena was served on Apple, Inc. for subscriber information pertaining to Bernhard Jakits, telephone number (443) 742-1792 and IMEI number 353824089666214. In response, Apple identified two Apple IDs, berniejakits@me.com and berniejakits@comcast.net as being associated with the provided information.

49. On April 14, 2020, a federal search warrant was obtained for the **SUBJECT ACCOUNTS.** The information provided by Apple in response to the federal search warrant for the **SUBJECT ACCOUNTS** revealed numerous images of Victim 1 and Victim 2 stored in the content of the iCloud account as well as a photograph of Jakits' Maryland Driver's License showing a date of birth of 6/1/1951. Specifically, the following 17 images were found to be present in the account:

- Image 1 – Photograph of a young Hispanic female lying naked on a sheet displaying her breasts and vagina. Your affiant believes this to be Victim 1 based on a review of other known photographs of Victim 1. Furthermore, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 2 – Photograph of a young naked Hispanic female bent over an object, possibly a bed. Your affiant was unable to conclusively identify the female as either Victim 1 or Victim 2, but did find a similar photograph on Victim 1's cellular telephone and believes it is probable that the female in the photograph is either Victim 1 or Victim 2.
- Image 3 – Close up of a vagina. Your affiant was unable to identify the female, but did find a similar photograph on Victim 1's cellular telephone and believes it is probable that the female in the photograph is either Victim 1 or Victim 2.
- Image 4 – Photograph of a young Hispanic female laying naked on a sheet displaying her breasts and vagina. Your affiant believes this to be Victim 1 based on a review of other known photographs of Victim 1. Furthermore, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 5 – Photograph of a young Hispanic female squatting naked displaying her breasts and vagina. Your affiant believes this to be Victim 1. While the female's face is not captured in the image, a necklace similar in appearance to one worn by Victim 1 in other photographs is visible. Furthermore, your affiant found a similar photograph on Victim 1's cellular telephone.

- Image 6 – Photograph of a young Hispanic female displaying her exposed breasts. Your affiant believes this to be Victim 1. While the female's face is not captured in the image a necklace similar in appearance to one worn by Victim 1 in other photographs is visible. Furthermore, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 7 – Photograph of a young Hispanic female standing naked and showing her breasts. While the female's face is not captured in the photograph, text added to the image identifies the female photographed as Victim 1. Furthermore, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 8 – Photograph of a young Hispanic female posing naked in mirror with breasts exposed. Your affiant believes this to be Victim 1. While the female's face is partially obscured in the image. a necklace similar in appearance to one worn by Victim 1 in other photographs is visible. Furthermore, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 9 – Photograph of a young Hispanic female kneeling and wearing black bra and panties. Your affiant believes this to be Victim 1. While the female's face is obscured in the image, a necklace similar in appearance to one worn by Victim 1 in other photographs is visible. Additionally, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 10 – Close up photograph of a female's buttocks while wearing a black thong. Your affiant was unable to identify the female as either Victim 1 or Victim 2. However, your affiant observed a similar photograph on Victim 1's cellular telephone and believes it is probable that the female in the photograph is either Victim 1 or Victim 2.
- Image 11 – Close up photograph of a vagina. Your affiant was unable to identify the female as either Victim 1 or Victim 2. Your affiant found a similar photograph on Victim 1's cellular telephone and believes it is probable that the female in the photograph is either Victim 1 or Victim 2.
- Image 12– Photograph of a young Hispanic female kneeling and wearing black bra and panties. Your affiant believes this to be Victim 1. While the female's face is obscured in the image, a necklace similar in appearance to one worn by Victim 1 in other photographs is visible. Additionally, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 13 – Photograph of a young Hispanic female kneeling and wearing white bra and panties. Your affiant was unable to identify the female as either Victim 1 or Victim 2. Your affiant observed a similar photograph on Victim 1's cellular telephone and believes it is probable that the female in the photograph is either Victim 1 or Victim 2.
- Image 14 – Black and white photograph of a young female sitting on bathroom counter wearing thong panties. Although your affiant was unable to conclusively identify the female as either Victim 1 or Victim 2, a similar photograph was recovered from Victim 1's cellular telephone. Your affiant thus believes it is probable that the female in the photograph is either Victim 1 or Victim 2.
- Image 15 – Photograph of Victim 1 clothed displaying a school report card.
- Image 16 – Photograph of a young Hispanic female lying naked on a sheet

displaying her breasts and vagina. Your affiant believes this to be Victim 1 based on a review of other known photographs of Victim 1. Furthermore, your affiant found a similar photograph on Victim 1's cellular telephone.

- Image 17 – Photograph of a young Hispanic female posing in a mirror wearing a black bra with a floral pattern. Your affiant was unable to identify the female as either Victim 1 or Victim 2. Your affiant found a similar photograph on Victim 1's cellular telephone and believes it is probable that the female in the photograph is either Victim 1 or Victim 2.

50. All of these photos were identical to images recovered from Victim 1's phone, several of which had been sent to the grandmother's phone. Additional records obtained via subpoena to Western Union confirmed that Jakits paid for these photographs, sending $150 to Victim 1's grandmother on January 4 and $500 of January 11, 2019.

51. On June 16, 2020, your affiant conducted an interview of Victim 1 and A.M, to obtain further information regarding Victim 1's communications with Jakits. Victim 1 explained about that she would take photos on her phone, forward them to her grandmother's phone, and then use the grandmother's phone to send them to Jakits. Victim 1 would do this when her phone did not have minutes.

52. A search warrant for Jakits' residence in Maryland was obtained and executed in December of 2020. Upon the initial execution, it was discovered that Jakits was traveling to Los Angeles, CA at the time of the execution. Your affiant obtained Jakits' flight in formation, and upon his arrival at LAX, he was met by Agents of the FBI. Jakits consented to speak to the agents and provided them with an Apple iPhone, an Apple laptop computer, and an iPad, all of which he had brought with him from Maryland. He also consented to searches of his Apple laptop, and a subsequent manual review of the iPad led to the discovery of a photo vault application. When asked, Jakits provided the pass code for the photo vault application. In the application, FBI agents observed folders labeled with the names of Victim 1 and Victim 2. When FBI agents opened the folders, they observed sexually explicit photos of young females. A photo in the folder labeled with Victim 1's name showed a female holding what appeared to be a school transcript. A photo in the folder labeled with Victim 2's name depicted a female holding a piece of paper that displayed her date of birth, indicating her age as being 13 years old at the time the photograph was taken. The description of these images, as provided by the FBI agents in California who were observing them and relaying the information to your affiant at the time, is consistent with photos that Victim 1 and Victim 2 sent to Jakits, as observed in the chat log on Victim 1's phone and in Jakits' iCloud account.

53. After finding what they believed to be child pornography on Jakits' iPad, the LA FBI Agents seized all of Jakits' devices and shipped them from the Los Angeles FBI to the Cincinnati FBI for further review and forensic examination. Additionally, numerous computers, cellular phones, and external storage media were seized from Jakits' residence and subsequently shipped to the Cincinnati FBI office. Your affiant subsequently obtained a search warrant authorizing the forensic examination of the Apple iPad Pro Serial Number, DMPWG0FTHPT4, the Apple Laptop Serial Number, C17N6MT86085, and the Apple iPhone 12, serial number C392Q0T1N6XX, which were all seized from Jakits by the FBI agents in LA. Those devices, along with all of the devices seized from Jakits residence, including an Apple iMac Desktop Computer, serial number C02ZK1LCJWDX, were later forensically extracted by FBI forensics agents. Your affiant has reviewed the forensic extractions of all of the devices and located images of Victim 1 and Victim 2, including both clothed and nude or pornographic depictions, on all of the above noted devices.

54. Subsequent to the issuance of the indictment in this case, and in preparation for the impending trial, your affiant obtained a second search warrant for all of the devices that had been seized from Jakits' person and residence. This search warrant was based on an observation during the previous review of the devices of what appeared to be a video depicting A.M. engaged in bestiality, which corroborates what A.M. told your affiant about Jakits' extortion of her. Upon the issuance of the second search warrant, additional extractions and reviews of all of Jakits and the victims' devices were conducted by a forensically-trained FBI agent. That review revealed the presence of communications between A.M. and Jakits, as well as numerous videos of A.M. and other adult females engaged in sexual acts including bestiality. Jakits face was visible in these recordings, as it appears that he was utilizing one Apple device to record a video chat he was conducting on another Apple device. Jakits voice was also heard directing, and at times, ordering A.M. to engage in specific sexual acts with dogs. In certain videos, A.M. appeared to be in visible and audible distress. Evidence was also recovered that indicates Jakits sent A.M. videos or images of herself and other adult women engaged in bestiality.

55. The information recovered and reviewed from one of Jakits devices, specifically the Apple iMac Computer, also suggested that at least one additional device that is not in the government's possession had at one time also been synced to the **SUBJECT ACCOUNTS**. This information is corroborated by the initial review of the iCloud evidence which suggests

that the additional device was in use during the time period in which Jakits is alleged to have communicated with A.M. and/or her daughters, Victim 1 and Victim 2. Based on the new information that has been obtained from the execution of the additional search warrant for Jakits' devices, your affiant believes that there is additional evidence related to the extortion of A.M. and possibly other adult victims, as well as currently undiscovered evidence pertaining the exploitation of Victim 1 and Victim 2 contained within the **SUBJECT ACCOUNTS**.

VIII. CONCLUSION

56. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 875(d), 1465, 2251, 2252 and 2422(b) – interstate extortion, production of obscenity for interstate distribution, production, advertising/solicitation for, and receipt of visual depictions of minors engaged in sexually explicit conduct (hereinafter "child pornography"), and the coercion or enticement of a minor(s), have been committed, and evidence of those violations is located on the **SUBJECT ACCOUNTS**. Your affiant respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT ACCOUNTS** and the seizure of the items described in Attachment B.

Andrew D. McCabe
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 22nd day of December, 2022.

Kimberly A. Johnson
United States Magistrate Judge

)hio

ATTACHMENT A
Property to Be Searched

This warrant applies to the content of the iCloud accounts, including the content of communications, that are associated with the email accounts berniejakits@me.com and berniejakits@comcast.net (the **SUBJECT ACCOUNTS**) that was provided to the FBI by Apple, Inc. pursuant to a search warrant issued on April 14, 2020, and which has saved on a digital device and remained in secure evidence storage at the FBI Columbus, located at 425 West Nationwide Blvd., since its receipt by the FBI from Apple.

This warrant does not apply to any additional content located only on Apple's servers and does not require any further disclosure by Apple, Inc.

ATTACHMENT B

Particular Things to be Seized

1. The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18 U.S.C. § 875(d) (interstate extortion); 18 U.S.C. § 1465 (production of obscenity for interstate distribution); 18 U.S.C. § 2251(a) (production of child pornography); 18 U.S.C. § 2251(d) (notice for child pornography); 18 U.S.C. § 2252(a)(2) (receipt and distribution of child pornography); 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography); and 18 U.S.C. § 2422(b)(coercion and enticement):

a. Child pornography and child erotica.

b. Evidence of communications related to the production, possession, receipt, or distribution of child pornography and/or, the coercion or enticement of a minor to engage in illegal sexual activity.

c. Evidence that may identify any additional adult or minor victims, co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

d. Evidence the user possessed, exchanged, or requested visual depictions of minors, from other adults or minors themselves, whether clothed or not, for comparison to any child pornography or child erotica found during the execution of this search warrant or obtained during the course of this investigation.

e. Any and all chat, text, email, or other electronic communications regarding sexual activity with or by adults or minors, including information pertaining to the persons engaging in such communications, their identities, locations, and any money sent or received because of any sexual activities engaged in.

f. Any and all images and videos depicting sexually explicit activity, whether involving adults or minors.

g. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation.

h. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

i. Evidence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

j. Evidence of the lack of such malicious software.

k. Evidence indicating how and when the device was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user.

l. Evidence of the attachment to the device of other storage devices or similar containers for electronic evidence.

m. Evidence of programs (and associated data) that are designed to eliminate data from the device.

n. Evidence of the times the device was used.

o. Records of or information about Internet Protocol addresses used by the device.

p. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages,

search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

q. Contextual information necessary to understand the evidence described in this attachment.

r. Records, information, and items relating to violations of the statutes described above.

2. This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

3. With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

4. If after performing these procedures, the directories, files or storage areas do not reveal evidence of child pornography or other criminal activity, the further search of that particular directory, file or storage area, shall cease.